

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF INDIANA
HAMMOND DIVISION**

STATE OF INDIANA EX REL. ROKITA,

Plaintiff,

v.

CAREPOINTE, P.C.,

Defendant.

Case No. 2:23-cv-328

**COMPLAINT FOR INJUNCTIVE
RELIEF, DAMAGES, ATTORNEY
FEES AND COSTS**

REQUEST FOR JURY TRIAL

Plaintiff, Indiana Attorney General *ex rel.* Todd Rokita, as *parens patriae* for the residents of the State of Indiana (the “State”), by Deputy Attorney General Jennifer M. Van Dame, brings this action for injunctive relief, statutory damages, attorney fees, and costs against CarePointe, P.C. (“CarePointe”) for violations of the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.1936, as amended by the Health Information Technology for Economic and Clinical Health Act Pub. L. No. 111-5, 123 Stat. 226 (collectively, “HIPAA”), as well as the Indiana Disclosure of Security Breach Act, Ind. Code § 24-4.9 *et seq.* (“DSBA”) and Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 *et seq.* (“DCSA”), stemming from CarePointe’s deficient security practices contributing to a data breach affecting over 45,000 patients and CarePointe’s misrepresentations to patients regarding its security practices. In support of its Complaint, the State alleges:

I. PARTIES, JURISDICTION, AND VENUE

1. The Indiana Attorney General is authorized to bring this action to enforce HIPAA pursuant to 42 U.S.C. § 1320d-5(d). The Indiana Attorney General is authorized to bring this action to enforce the DSBA pursuant to Ind. Code § 24-4.9-4-2, and the DCSA pursuant to Ind. Code § 24-5-0.5-4(c).

2. CarePointe, P.C. (“CarePointe”) is an Indiana professional corporation with a principal office located at 99 E 86th Ave, Suite A, Merrillville, IN 46410.

3. This Court has jurisdiction pursuant to 42 U.S.C. § 1320d-5(d)(1) and 28 U.S.C. § 1331. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C § 1367.

4. Venue in this District is proper pursuant to 28 U.S.C. § 1391(b)(1) and (b)(2).

5. The State has provided notice of this action to the Secretary of Health and Human Services as required under 42 U.S.C. §1320d-5(d)(4).

II. FACTUAL ALLEGATIONS

6. At all times relevant to this Complaint, CarePointe provided health care services to Indiana residents and was a covered entity within the meaning of HIPAA. *See* 45 C.F.R. § 160.103.

7. On or around June 25, 2021, sensitive patient information was exfiltrated from CarePointe’s systems during a ransomware event (the “Data Breach”).

8. CarePointe provided notification of the Data Breach to patients and the

State on August 23, 2021.

9. The Data Breach exposed the personal information and/or protected health information (“PHI”) of approximately 45,002 Indiana residents.

10. The categories of personal information and/or PHI exposed by the Data Breach included: names, addresses, dates of birth, Social Security numbers, medical insurance information, and health information.

11. CarePointe’s Notice of Privacy Practices (effective March 24, 2003),¹ touts “OUR COMMITMENT TO PROTECTING HEALTH INFORMATION ABOUT YOU”, stating:

- a. “We consider it our great privilege to serve your medical needs and we value the trust you have placed in us. We are committed to safeguarding your patient information . . .”;
- b. “The HIPAA Privacy Rule requires that we protect the privacy of health information that identifies a patient . . .”; and
- c. “We are required by law to: Maintain the privacy of PHI about you . . .”

12. Moreover, CarePointe’s Notice of Privacy Practices Acknowledgement,²

¹ Notice of Privacy Practices, CarePointe Ear, Nose, Throat and Sinus Centers, *available at* https://carepointe.net/wp-content/uploads/2016/05/Notice_of_Privacy_Practices.pdf (last accessed Sept. 22, 2023).

² Notice of Privacy Practices Acknowledgement, *available at* https://carepointe.net/wp-content/uploads/2016/07/Notice_of_Privacy_Practices-Acknowledgement.pdf (last accessed Sept. 22, 2023).

requires patients to acknowledge that they have “received, read and understand” CarePointe’s Notice of Privacy Practices and certify: “I understand that, under the Health Insurance Portability & Accountability Act of 1996 (“HIPAA”), I have certain rights to privacy regarding my protected health information.”

13. Notwithstanding CarePointe’s representations regarding its commitment to patient privacy in its Notice of Privacy Practices and Notice of Privacy Practices Acknowledgement, CarePointe lacked appropriate security policies, failed to conduct appropriate risk assessments, and failed to promptly address known security issues.

14. In or around late 2020, CarePointe had initial meetings with an IT vendor who flagged CarePointe’s remote access policies as a security issue that needed to be addressed (the “IT Vendor”).

15. By January 2021, the IT Vendor completed a written HIPAA risk assessment that put CarePointe on notice of many additional security issues that contributed to the Data Breach later that year, including:

- a. Weak password policies, including no password expiration, passwords of less than 8 characters allowed, and no password complexity requirement;
- b. Account lockout after a number of failed login attempts disabled;
- c. Active Directory contained inactive/decommissioned computers;
- d. A number of users not logged in for an extended period indicating a lack of procedures for terminating user access;

- e. Outdated anti-virus software;
- f. Unrestricted access rights to network shares containing PHI; and
- g. Use of generic logins for systems containing PHI.

16. CarePointe eventually hired the IT Vendor in March 2021 to address the security issues flagged in the January 2021 HIPAA risk assessment, but the work was not completed before the Data Breach in June 2021.

17. CarePointe did not move quickly enough to address the significant risks that had developed after years of poor security practices.

18. The threat actor who deployed ransomware on CarePointe's systems gained access from outside of CarePointe's network via an open, unsecured port used for remote access.

19. The security issues flagged by the IT Vendor allowed the threat actor to infiltrate CarePointe's network undetected, exfiltrate patient data, and execute ransomware to fully encrypt all systems.

20. If CarePointe had maintained appropriate security policies, conducted appropriate risk assessments, and implemented a risk management plan to mitigate the risks identified by the risk assessments, as required by HIPAA, the obvious and significant security issues flagged by the IT Vendor in late 2020 and early 2021 would have been identified and addressed sooner.

21. CarePointe also failed to execute a business associate agreement with the IT Vendor until April 29, 2021, *after* the IT Vendor received access to CarePointe's systems to complete the January 2021 HIPAA risk assessment.

22. The IT Vendor also flagged the use of public domain email accounts such as MSN for CarePointe business, which continued through April 2022.

III. HIPAA BACKGROUND

23. As a covered entity, CarePointe was required to comply with the HIPAA standards that govern the privacy and security of PHI. *See* 45 C.F.R. Part 164.

24. The HIPAA Security Rule (45 C.F.R. Part 164, Subpart C) requires covered entities to ensure the confidentiality, integrity, and availability of all PHI that the covered entity creates, receives, maintains, or transmits and to protect against any reasonably anticipated threats to the security or integrity of such information. *See* 45 C.F.R. § 164.306. To this end, the HIPAA Security Rule requires covered entities to employ appropriate administrative, physical, and technical safeguards to maintain the security and integrity of PHI. *See* 45 C.F.R. §§ 164.308, 164.310, 164.312.

25. It is the covered entity's responsibility to ensure compliance with HIPAA, including the Security Rule. A covered entity may delegate its obligations under the Security Rule to a business associate, such as an IT vendor, but the covered entity is liable for an agent's failure to comply with the Security Rule. *See Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act*, 78 FR 5580-5581 (Jan. 25, 2013).

26. Finally, the HIPAA Privacy Rule (45 C.F.R. Part 164, Subpart E) prohibits covered entities from using or disclosing PHI, except as permitted by HIPAA.

IV. CAUSES OF ACTION

COUNT ONE: FAILURE TO COMPLY WITH HIPAA SECURITY RULE

27. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

28. The State investigated CarePointe's compliance with the Security Rule after CarePointe notified the State of the Data Breach.

29. Leading up to the Data Breach, CarePointe failed to employ appropriate safeguards to maintain the security and integrity of PHI, including as follows:

- a. CarePointe failed to implement, review, and/or modify policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §§ 164.308(a)(1)(i) and 164.306(e);
- b. CarePointe failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- c. CarePointe failed to implement procedures for terminating access to PHI when the employment of, or other arrangement with, a workforce member ends or as required, or reasonable and appropriate alternatives to such procedures with documentation in violation of 45 C.F.R. § 164.308(a)(3)(C);
- d. CarePointe failed to implement procedures for guarding against, detecting, and reporting malicious software, or reasonable and

appropriate alternatives to such procedures with documentation in violation of 45 C.F.R. § 164.308(a)(5)(ii)(B);

- e. CarePointe failed to implement procedures for monitoring log-ins, or reasonable and appropriate alternatives to such procedures with documentation in violation of 45 C.F.R. § 164.308(a)(5)(ii)(C);
- f. CarePointe failed to implement procedures for creating, changing, and safeguarding passwords, or reasonable and appropriate alternatives to such procedures with documentation in violation of 45 C.F.R. § 164.308(a)(5)(ii)(D);
- g. CarePointe failed to implement technical policies and procedures for electronic information systems that maintain PHI to allow access only to those persons that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- h. CarePointe failed to assign unique names and/or numbers for identifying and tracking user identity in violation of 45 C.F.R. § 164.312(a)(2)(i);
- i. CarePointe failed to implement a mechanism to encrypt PHI at rest, or reasonable and appropriate alternatives to such mechanisms with documentation in violation of 45 C.F.R. § 164.312(a)(2)(iv);
- j. CarePointe failed to implement procedures to verify that a person seeking access to PHI is the one claimed in violation of 45 C.F.R. § 164.312(d).

- k. Prior to January 2021, CarePointe failed to conduct accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by CarePointe in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A);
 - l. Prior to January 2021, CarePointe failed to implement a risk management plan that applies security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B); and
 - m. CarePointe failed to execute an appropriate business associate agreement with its IT Vendor until *after* the IT Vendor received access to CarePointe's systems to complete a HIPAA risk assessment in violation of 45 C.F.R. § 164.308(b).
30. Each security issue identified in Paragraph 29, Subparagraphs (a)-(m) is a separate, continuing violation of the Security Rule that arose before the Data Breach.
31. For continuing violations, 42 U.S.C. § 1320d-5(d)(2) and 45 C.F.R. § 160.406 authorize statutory damages of \$100 per HIPAA violation, per day, totaling up to \$25,000 per year for violations of an identical requirement or prohibition.

**COUNT TWO:
FAILURE TO COMPLY WITH HIPAA PRIVACY RULE**

32. The State incorporates by reference all preceding paragraphs as if fully set forth herein.
33. As a covered entity, CarePointe was prohibited from disclosing PHI

except as permitted by HIPAA. 45 C.F.R. § 164.502(a).

34. HIPAA defines “disclosure” as “the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.” 45 C.F.R. § 160.103.

35. CarePointe’s deficient security practices subjected the PHI of approximately 45,002 Indiana residents to disclosure during the Data Breach.

36. The disclosures were not permitted under any HIPAA exception.

37. Each disclosure was a separate violation of the Privacy Rule.

38. 42 U.S.C. § 1320d-5(d)(2) and 45 C.F.R. § 160.406 authorize statutory damages of \$100 per HIPAA violation, totaling up to \$25,000 per year.

**COUNT THREE:
FAILURE TO IMPLEMENT AND MAINTAIN
REASONABLE PROCEDURES IN VIOLATION OF
INDIANA DISCLOSURE OF SECURITY BREACH ACT**

39. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

40. The DSBA requires a data base owner to “implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner.” Ind. Code § 24-4.9-3-3.5(c).

41. The DSBA defines “personal information” to include:

- (1) a Social Security number that is not encrypted or redacted; or
- (2) an individual’s first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:

- (A) A driver's license number.
- (B) A state identification card number.
- (C) A credit card number.
- (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

Ind. Code § 24-4.9-2-10.

42. The categories of personal information exposed by the Data Breach included names and Social Security numbers.

43. CarePointe violated the DSBA by failing to implement and maintain reasonable security procedures to protect and safeguard personal information of Indiana residents.

44. CarePointe is not exempt from the DSBA because CarePointe was not in compliance with HIPAA at the times relevant to this Complaint. *See* Ind. Code § 24-4.9-3-3.5(a).

**COUNT FOUR:
VIOLATIONS OF INDIANA DECEPTIVE CONSUMER SALES ACT**

45. The State incorporates by reference all preceding paragraphs as if fully set forth herein.

46. The DCSA regulates unfair, abusive, and/or deceptive acts, omissions, and/or practices between suppliers and consumers engaging in consumer transactions. *See* Ind. Code § 24-5-0.5-3.

47. Under the DCSA, a “consumer transaction” includes services and other intangibles. Ind. Code § 24-5-0.5-2(a)(1).

48. In supplying Indiana patients with health care services, CarePointe regularly engages in consumer transactions in Indiana and is a “supplier” as defined

by Ind. Code § 24-5-0.5-2(a)(3).

49. The DCSA prohibits a supplier from committing “an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction . . . whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations.” Ind. Code. § 24-5-0.5-3(a).

50. It is a deceptive act under the DCSA to represent to consumers that the subject of a consumer transaction “has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have,” or “is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not.” Ind. Code § 24-5-0.5-3(b)(1)-(2).

51. In its Notice of Privacy Practices, CarePointe represented to patients that it is committed to “PROTECTING HEALTH INFORMATION ABOUT YOU”, stating: “We consider it our great privilege to serve your medical needs and we value the trust you have placed in us. We are committed to safeguarding your patient information . . . ”

52. CarePointe also implicitly represented that it is compliant with HIPAA and other applicable laws by:

- a. Stating its Notice of Privacy Practices: “The HIPAA Privacy Rule requires that we protect the privacy of health information that identifies a patient . . . ”; and “We are required by law to:

Maintain the privacy of PHI about you . . . ”; and

- b. Requiring patients to certify in its Notice of Privacy Practices Acknowledgement: “I understand that, under the Health Insurance Portability & Accountability Act of 1996 (“HIPAA”), I have certain rights to privacy regarding my protected health information.”

53. Contrary to these representations, CarePointe knowingly failed to implement and maintain reasonable security practices to protect patients’ PHI.

54. CarePointe also knowingly failed to comply with HIPAA by failing to promptly address the security issues flagged by its IT Vendor in late 2020 and early 2021.

55. CarePointe explicitly and implicitly misrepresented that its systems were secure and compliant, when CarePointe knew they were not.

56. CarePointe knowingly committed unfair, abusive, and/or deceptive acts, omissions, and/or practices in connection with consumer transactions in violation of the DCSA, subjecting it to a civil penalty of up to \$5,000 per violation under Ind. Code § 24-5-0.5-4(g).

V. PRAYER FOR RELIEF

WHEREFORE, the State of Indiana respectfully requests that this Court enter judgment against CarePointe and in favor of the State as follows:

- a. Finding that CarePointe violated HIPAA, DSBA, and DCSA by engaging in the unlawful acts and practices alleged herein, and permanently enjoining

CarePointe from continuing to engage in such unlawful acts and practices pursuant to 42 U.S.C. § 1320d-5(d)(1)(A), Ind. Code § 24-4.9-3-3.5(f), and Ind. Code § 24-5-0.5-4(c);

b. Ordering CarePointe to pay statutory damages of \$100 per HIPAA violation, per day, totaling up \$25,000 per year for violations of an identical requirement or prohibition, as provided by 42 U.S.C. § 1320d-5(d)(2) and 45 C.F.R. § 160.406;

c. Ordering CarePointe to pay a \$5,000 civil penalty for violating the DSBA, as provided by Ind. Code § 24-4.9-3-3.5(f);

d. Ordering CarePointe to pay a \$5,000 civil penalty for each knowing violation of the DCSA alleged herein, as provided by Ind. Code § 24-5-0.5-4(g);

e. Ordering CarePointe to pay all costs and fees for the investigation and prosecution of this action pursuant to 42 U.S.C. § 1320d-5(d)(3), Ind. Code § 24-4.9-3-3.5(f), and Ind. Code § 24-5-0.5-4(c); and

f. Granting any such further relief as the Court may deem appropriate.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury of all issues so triable.

Respectfully submitted,

STATE OF INDIANA EX REL.
INDIANA ATTORNEY GENERAL
TODD ROKITA

Date: September 29, 2023

/s/ Jennifer M. Van Dame

Jennifer M. Van Dame
Indiana Attorney No. 32788-53
Deputy Attorney General
Data Privacy & Identity Theft Unit
Office of the Indiana Attorney General
302 West Washington Street
Indianapolis, IN 46037
Phone: 317-232-0486
Fax: 317-232-7979
Email: jennifer.vandame@atg.in.gov